[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 12/14
G06F 13/36 G06F 11/00
G06F 17/30 G06F 15/173

[12]发明专利申请公开说明书

[21]申请号 99805972.2

[43]公开日 2001年8月15日

[11]公开号 CN 1308745A

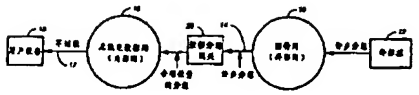
[22]申请日 1999.4.1 [21]申请号 99805972.2
[30]优先权
[32]1998.5.8 [33]US [31]09/075,289
[86]国际申请 PCT/US99/07235 1999.4.1
[87]国际公布 WO99/59071 英 1999.11.18
[85]进入国家阶段日期 2000.11.8
[71]申请人 摩托罗拉公司
地址 美国伊利诺斯
[72]发明人 托马斯·韦恩·洛克哈特
卡尔·安东尼·里尔登
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 酆 迅

权利要求书3页 说明书6页 附图页数4页

[54]发明名称 保护网络避免数据分组过载的方法

[57]摘要

保护一个内部网(16)免于受到来源于外部网(10)中来源的过量数据分组所造成的过载。在优选实施例中,数据分组网关(20)接收每个输入数据分组及判断它是否来自可靠源。如果它不是来自可靠源,及最近从同一来源接收的数据分组数量超过一个阈值,则摒弃来自该来源的数据分组。当来自所有不可靠来源的输入数据分组超过另一个阈值时,最好摒弃来自所有不可靠来源的更多数据分组。



ISSN1008-4274

权 利 要 求 书

1.一种用于在通信系统中保护用户免于接收过量的来源于外部网中分组源的数据分组的方法，该通信系统所具有的内部网通过通信线路自该分组源接收数据分组以便进一步传输至内部网中的用户，该方法包括以下步骤:

a)在通信线路内建立一个数据分组网关，并且在该数据分组网关处:

b)接收一个数据分组及识别其分组源;

c)为该识别的分组源将分组计数增量;

d)如果分组计数超过一个阈值则摒弃该数据分组；及

e)如果分组计数低于该阈值则将该数据分组送至内部网。

2.如权利要求1中提出的方法，其中如果步骤b)识别一个分组源为多个所选源中的一个，则不论先前自同一所选源收到的数据分组数量多少，都将自该处收到的数据分组发送至内部网。

3.如权利要求2中提出的方法，其中所选源是可靠分组源，及其中所有来自可靠分组源的分组都送至内部网。

4.如权利要求1中提出的方法，包括:

f)当收到一个数据分组时将总分组计数增量；及

g)当增量的总分组计数超过一个允许的总分组计数时摒弃收到的数据分组。

5.如权利要求1中提出的方法，其中一个数据分组包括一个源地址，该方法还包括建立一个用于存储源地址的地址表及将收到的数据分组的源地址与存于地址表中的源地址进行比较的步骤。

6.如权利要求5中提出的方法，其中如果收到的数据分组的源地址与存于地址表中的地址不匹配，及如果该地址表没有用于接收另一个源地址的空间，则摒弃该收到的数据分组。

7.如权利要求6中提出的方法，其中如果收到的数据分组的源地址与存于地址表中的地址不匹配，及如果该地址表具有用于接收另一个源地址的空间，则将收到的数据分组的源地址存于地址表中。

8.如权利要求1中提出的方法，其中在预定时间周期内收到数据分组时将识别的分组源的分组计数增量，以及在预定时间周期外将每个分组计数按照预定系数减少。

9.如权利要求8中提出的方法还包括建立一个用于存储已经自其中收到数据分组的源地址的地址表，以及其中如果源地址的减少的分组计数低于释放阈值，则将该源地址自地址表中删去。

10.一种用于在系统中保护接收机免于接收过量的来源于因特网源的数据分组的方法，该系统内所具有的通信网络通过通信线路自因特网源接收数据分组以便进一步传输至通信网络中的接收机，该方法包括以下步骤:

a)在通信线路内建立一个数据分组网关，并且在该数据分组网关处:

b)接收一个具有因特网源地址的数据分组;

c)将与该因特网源地址相关连的第一分组计数增量;

d)将用于表示自至少某些因特网源地址收到的数据分组总计数的第二分组计数增量; 及

e)如果或者第一分组计数超过第一阈值，或者第二分组计数超过第二阈值，则摒弃该数据分组。

11.如权利要求10中提出的方法，其中如果步骤b)中所涉及的因特网源地址是多个可靠源中的一个，则不论先前自同一可靠源收到的数据分组数量多少，都接收自该处收到的数据分组。

12.如权利要求10中提出的方法，其中在预定时间周期内收到数据分组时将每个识别的分组源的分组计数增量，以及在预定时间周期外将每个分组计数按照预定系数减少.

13.如权利要求12中提出的方法还包括建立一个用于存储已经自其中收到数据分组的源地址的地址表的步骤，以及其中如果源地址的减少的分组计数低于释放阈值，则将该源地址自地址表中删去。

14.如权利要求10中提出的方法，其中该通信网络是一个传呼网络.

15.如权利要求10中提出的方法，其中该通信网络是一个无线电数据网络。

16.一种用于在通信系统中保护接收机免于接收过量的来源于因特网源的数据分组的方法，该通信系统内传呼网络通过通信线路自因特网源接收数据分组以便进一步传输至传呼网络中的接收机，该方法包括以下步骤:

a)在通信线路内建立一个数据分组网关，并且在该数据分组网关处:

b)接收一个具有因特网源地址的数据分组;

c)将该因特网源地址与所选源地址表进行比较;

d)如果因特网源地址不在所选源地址表内:

e)则将与该因特网源地址相关连的第一分组计数增量;

f)将用于表示自那些不在所选源地址表中的因特网源地址接收的数据分组总计数的第二分组计数增量；及

g)如果或者第一分组计数超过第一阈值，或者第二分组计数超过第二阈值，则摒弃该数据分组。

说　　明　　书

保护网络避免数据分组过载的方法

本发明涉及对来源于外部网例如因特网的数据分组的处理，及涉及在内部网中操作的用户。

如果大量数据分组自外部网输入至内部通信网络中的用户，内部网可能过载。现在使用因特网作为外部网例子来解释此问题，其中因特网能够发送极大量数据分组，而这些数据分组能够严重地阻碍内部网例如无线电数据网或传呼网络的工作。

因特网用户现在能够发送消息至在无线电网络中运行的个别无线电接收机。消息从因特网源出发，然后以数据分组形式发送至无线电网络。无线电网络将收到的数据分组发射至收信者的无线电接收机。

如果因特网源发射过量数据分组至无线电网络中的接收机，则无线电网络的出网信道将会阻塞，同时收信的无线电接收机将会收到大的帐单。这类对无线电网络的攻击可能是有目的或非故意的，例如由废弃邮件的发送者所造成。在以上任何一种情况下，其结果是无线电网络服务质量的下降，及数据分组的不情愿的接收者支付大帐单。

因特网与无线电网络之间的防火墙是用于保护无线电网络免受以上描述类型侵犯的传统机理。然而，传统防火墙也限制合法用户的任意接入。此外，即使通过防火墙，某些形式的攻击例如废弃电子邮件也能成功。传统的分组筛选可以保护网络，但它也能限制合法用户的接入。其他形式的能够发送大量数据分组至内部网中用户的外部网也有类似问题。

图1阐述传统通信系统，其中外部网例如因特网发射过量数据分组至内部网，其结果是在内部网是无线电数据网的情况下导致RF（射频）过载；

图2阐述用于在图1系统中用于根据本发明选择性地限制通过内部网的数据分组数量的数据分组网关的使用；

图3是用于显示数据分组网关的更多细节的框图；

图4是用于阐述数据分组网关如何优选地根据本发明进行分组处理操作的流程图；及

图5是用于阐述数据分组网关如何优选地执行清除过程的流程图。

参照图1，外部网10例如因特网自外部源12接收数据分组。外部源12通常是个人计算机、计算机服务器或其他能够生成数据分组的设备。所有这些设备有时在此处称为分组源。

这些数据分组（未示出）通常包括至少一个首部和一个信息段。首部包括例如源地址即分组源（外部源）12的地址、目的地址、路由信息等信息。信息段包括所有或部分待发送至所需目的地的消息。

如上所述，外部源12可能希望发送大量数据分组至另一个网络中的一个或多个收信者。如果这些收信者是无线电数据网的一部分，则无线电网络的出网信道可能阻塞，因而严重地阻碍网络运行。

在图1中，由源12生成的数据分组通过因特网10和通信线路14发送至内部网16，例如无线电数据网。此处所用名词“内部网”意味着用于服务于若干用户及无限制地自一个用户传输信息至另一个用户的通信网络；内部网也能在其内部用户与在内部网之外的其他网络之间传输信息。这类其他网络此处称为“外部网”，因为从内部网16的观点看，它们是“外部世界”的一部分。

由内部网16收到的数据分组通过线路17发射至收信的用户设备18。在内部网是无线电数据网的情况下，用户设备可以是通过RF线路与内部网通信的无线电接收机。用户设备的其他形式包括调制解调器、个人计算机和其他能够通过线路17与网络16通信的设备，线路17可以是RF、有线、或其他合适形式的通信线路。

当自外部网10接收过量数据分组时，图1中所示传统布置能够允许在线路17中出现RF过载。此问题可以根据本发明按照以下所述来解决：在外部网10与内部网16之间的线路14中建立一个数据分组网关20（图2），用于判断输入数据分组是否在所选（可靠的）来源清单之内，以及如果不在所选清单之内及如果自该来源的数据分组数量大于一个阈值数，则摒弃该数据分组。所有自选择清单中的来源收到的数据分组都通过并送至内部网。以此方式，将都通过并送至内部网的输入数据分组都通过并限制为内部网能够处理而不会不适当地降低其操作质

量的数量。数据分组网关20的这种操作模式及其操作的其他特征将在下面全面地描述。

现参照图3，数据分组网关20包括一个用于自内部网16接收数据分组的输入缓存22。在以传统方式存入缓存后，数据分组通过24处送至传统输出缓存26及自此处发射至外部网10以便分布至合适的外部源12。因此，来源于内部网16的数据分组发射至外部网中的它们的目的地而没有限制或修改。

来源于外部网10的数据分组由传统输入缓存28接收，然后经受外部分组处理过程30，这将在下面详细地描述。有把握说，过程30能将所选输入数据分组加以摒弃而避免内部网中阻塞。在处理后，被准许进入内部网的数据分组即送至传统输出缓存32。存入缓存的数据分组送至内部网16的输入端，内部网16根据包括于每个数据分组中的目的地址将分组分布至合适的用户设备18。

数据分组网关20还包括一个源地址表34，一个总分组计数器36和一个用于启动周期清除过程40的周期定时器38。单元34、36和38的功能在下面结合图4和5详细地描述。过程30和40最好由传统的微处理器或计算机执行，该微处理器或计算机如图4和5中的流程图所示地编程。

图4显示应用于每个由外部网发送的和由网关20接收的数据分组的过程（由图3中参考数字30所标示）。图4中某些注释是具体地针对因特网的，但此过程的实质可用于处理来自任何外部网的数据分组。

在第一步42，判断输入数据分组是否具有一个存于源地址表34（图3）中的IP（因特网协议）地址。表34是一个存储器，用于存储数据分组源地址，例如外部源12的地址和送至内部网16的数据分组的任何来源的源地址。最好在第一次从该特定来源接收数据分组的情况下就首先在表34中存储源地址。

如果该IP地址早已存储于表34中，则过程进至步骤44以便判断IP地址是否在所选可靠来源清单中，该可靠来源清单是一个合法数据分组源清单，预料这些数据分组源不会用无用数据分组塞满内部网，同时被允许无限制地发送数据分组至内部网。该清单可以存储于用于存储源地址表34的存储器的一部分内或存储于单独的传统存储器内。

如果通过步骤44判断收到的数据分组为来自可靠来源，则程序进至步骤46，其中接收该分组以便将它分布至其准备发送的用户18。此程序然后在步骤48退出，直至下一个来自外部网的数据分组到达，于是处理过程重新在步骤42处开始处理下一个输入数据分组。

如果在表34中找不到输入数据分组的IP地址（步骤42），则过程进至步骤50以便判断源地址表34是否具有空间用于接收另一个源地址入口。如果源地址表34没有用于另一个入口的空间，则在步骤52处删去被处理的数据分组，及程序在步骤54处退出。

如果在执行步骤50中发现表34具有用于另一个源地址入口的空间，则过程自步骤50进至步骤56以便将数据分组的IP地址输入至源地址表34中。在下一步58，将收到的数据分组注释为来自特定IP源，以及设置一个标志以便标示该特定IP源已经发送一个数据分组至内部网。

根据本发明的一个方面，为每个在最近周期内发送数据分组至内部网的IP源保持一个最近分组计数，其中一个周期是网关20接收输入数据分组时所用数分钟或数小时的时间周期。在下一个步骤60，将当今IP源的最近分组计数增加1.

本过程也保持一个表示用于将所有收到的数据分组进行计数的计数。此计数保持于总分组计数器36内（图3）。如果该总计数超过预定上限，则将要摒弃来自所有不可靠来源的数据分组。此操作能保护内部网免受智能形式的过载攻击，其中会修改路由器或其他设备而发送大量具有不同源地址的数据分组。

再参照图4，步骤62将总分组计数增加1。在下一步64，判断（此特定IP地址的）最近分组计数是否超过预定阈值。如果回答肯定，则过程进至步骤66，其中删去该数据分组，然后进至步骤68以便退出该程序。

如果对步骤64的回答否定，则程序进至步骤70，其中判断总分组计数（已在步骤62中增加1）是否超过其阈值。如果回答否定，则接收该分组（步骤46）。否则在步骤66处删去该分组。

为网关20接收的每个数据分组都执行图4中所示程序。因此，在一段时间之后源地址表34将会填满，及最近分组计数（步骤60）将会事

实上到达其阈值。因此，最好在执行图4中所示程序一段时间周期（例如15分钟周期）之后完成一个“清除”过程。此顺序周期地重复，在每个执行图4中所示数据分组处理过程的周期之后跟随一个清除过程。

现在参照图5，所阐述的流程图显示为每个存于源地址表34中的源地址执行清除过程。该过程于步骤72处开始以便判断所检查的源地址是否为可靠源地址。如果回答肯定，则此过程即完成（步骤74），并且不再进行操作。对于表34中下一个源地址，过程再在步骤72处开始。如果下一个源地址不是可靠源，则下一步76询问在上一个周期内是否从此特定源地址收到一个数据分组。如果回答否定，则从源地址表34中删去此源地址，并且释放它在存储器内的位置以便用于存储新源地址（步骤78），以及过程在步骤80中断。

回至步骤76，如果在上一个周期内收到来自所检查源地址的数据分组，则过程进至步骤82。在步中将该源地址的最近分组计数除以2。在下一步84，判断减半的最近分组计数是否小于一个释放阈值，该释放阈值表示一个相对低的计数，这是上一个周期内操作很少的特征。如果回答肯定，则将源地址删去并且释放它的位置以便在下一个周期内用于存储不同源地址。如果回答否定，则将源地址保持为表34中的一个入口，并且在步骤86清除其分组收到标志。（此标志是在图4的步骤58中设置的，在图5的步骤76中测试的）。

因此，每一个在上一个周期内相对地活跃的源地址在源地址表34中保持其入口，及将其最近分组计数减半以便允许在下一个周期内接收更多数据分组而不超过步骤64中的阈值（图4）。完全不活跃或不够活跃以致达不到释放阈值的源地址将从源地址表34中删去以便为后随周期内成为活跃的其他源地址释放空间。

再回来参照步骤82，来源的最近分组计数是否除以2并不重要。它可以除以任何数N，或者按照预定系数减少。

以上所述方法提供一个保镖，它阻止由于外部网发射过量数据分组至内部网而导致的意外的或有意的内部网溢出。此技术对于保护RF通信网络例如无线电数据网络和传呼网络免受利用因特网来自一个IP源的数据分组攻击特别有效，因为这些网络的出网信道很容易阻塞。在保护传呼网络的情况下，数据分组网关可以置于传呼终端上。分组

网关也可是一个独立设备或者可以位于其他设备内例如网络代理或防火墙内。

虽然已用优选实施例的形式说明了本发明，但熟悉技术的人显然了解，可在不背离本发明的情况下作出不同更动和修改。因此，认为所有这些更动和修改是在由所附权利要求书所定义的实质和范围之内。

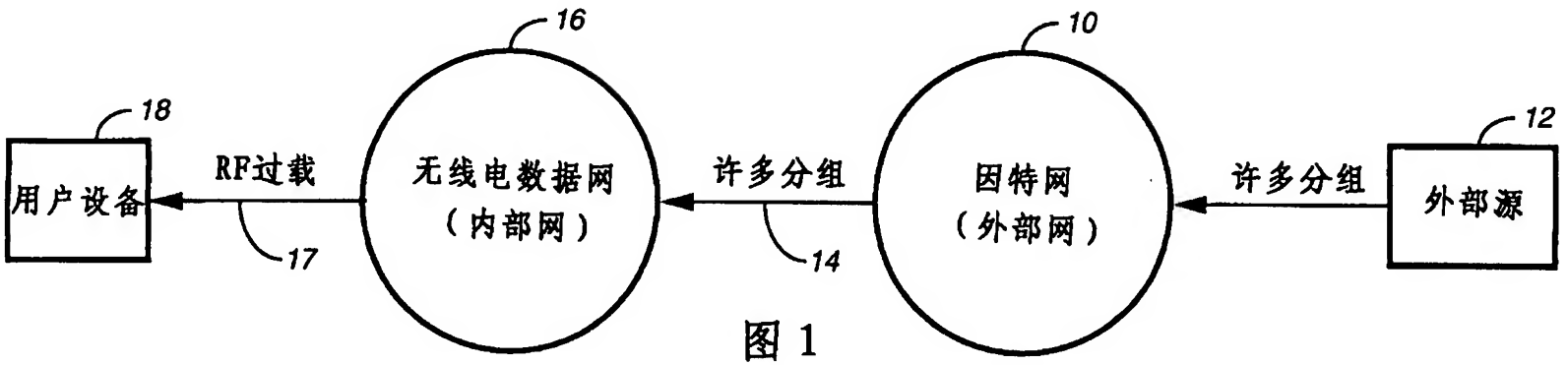

16
10
18
12
用户设备
RF过载
无线电数据网
（内部网）
许多分组
因特网
（外部网）
许多分组
外部源
17
14

图 1
现有技术

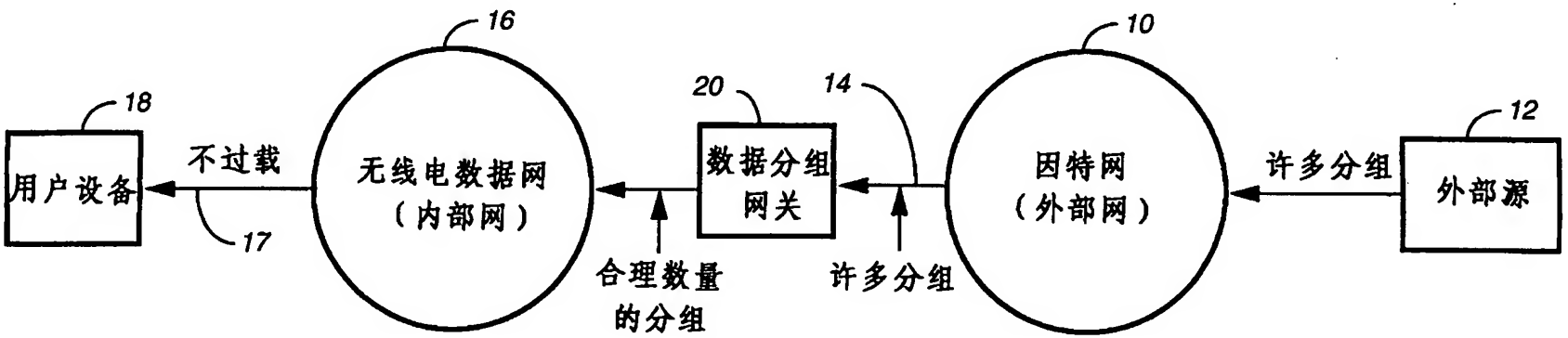

16
10
18
20
14
12
用户设备
不过载
无线电数据网
（内部网）
数据分组
网关
因特网
（外部网）
许多分组
外部源
17
合理数量
的分组
许多分组

图 2

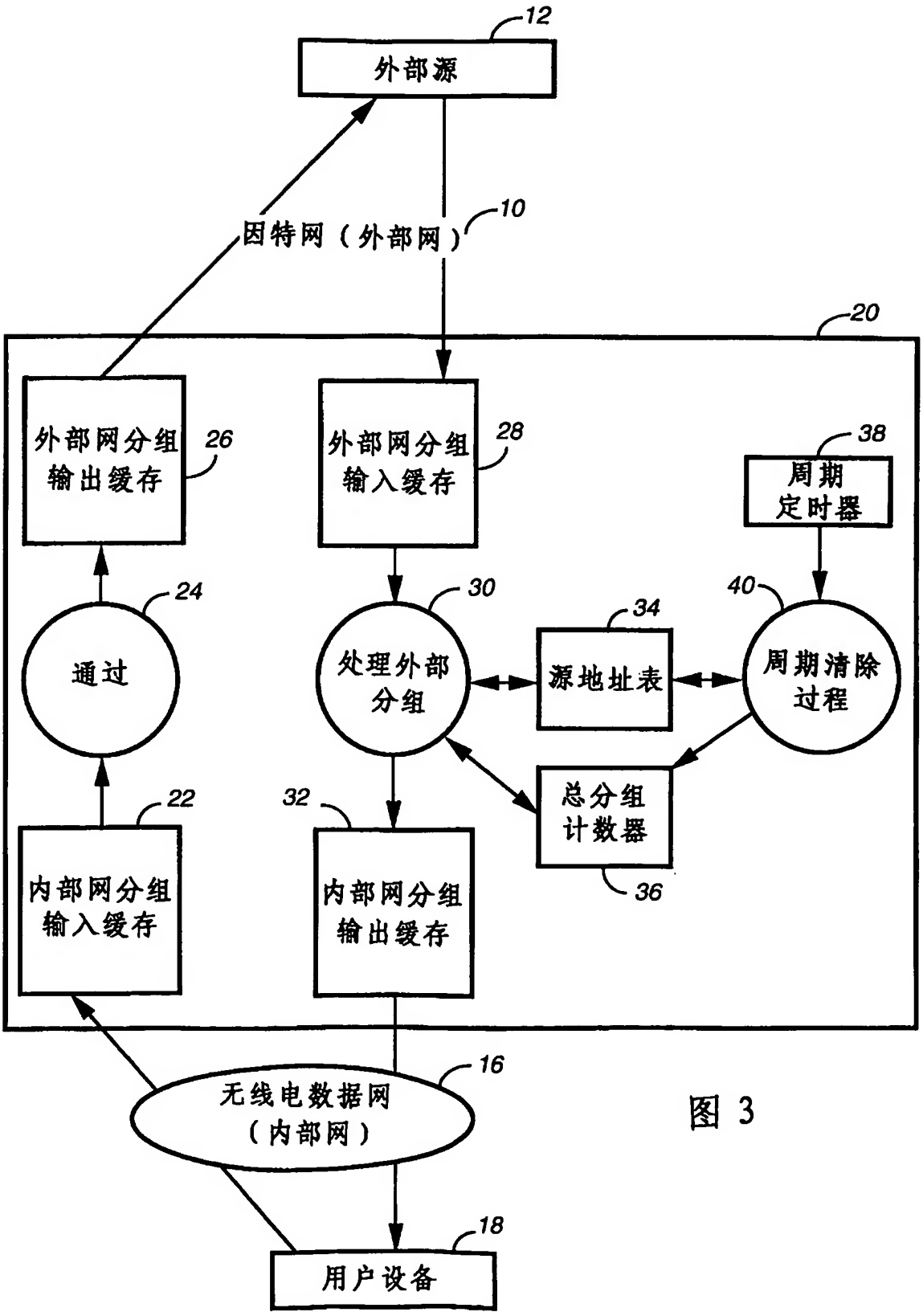

12
外部源
10
因特网（外部网）
20
外部网分组输出缓存
26
外部网分组输入缓存
28
周期定时器
38
24
通过
30
处理外部分组
34
源地址表
40
周期清除过程
总分组计数器
36
22
内部网分组输入缓存
32
内部网分组输出缓存
16
无线电数据网（内部网）
18
用户设备

图 3

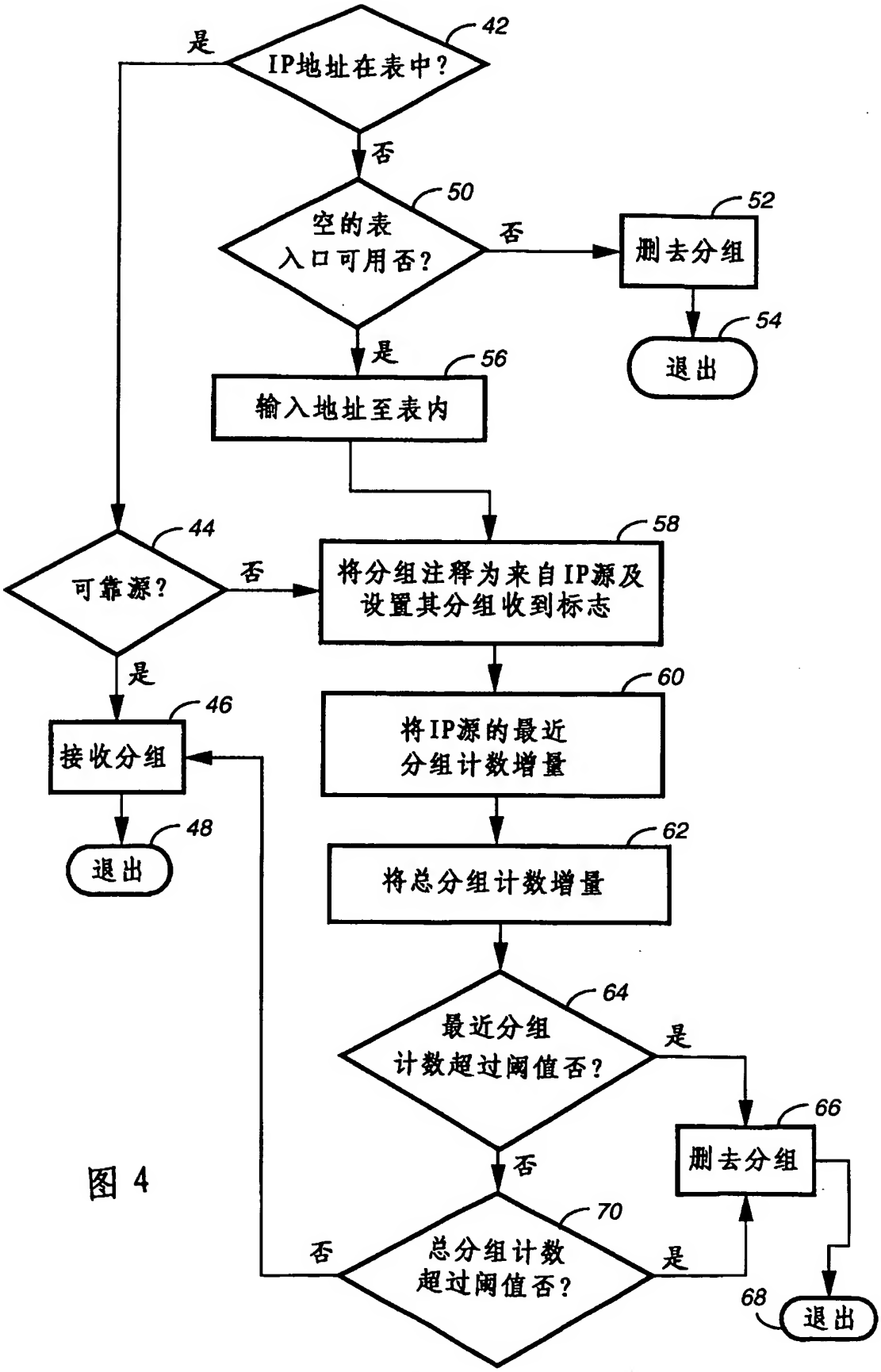

42
IP地址在表中？
是
否
50
空的表
入口可用否？
否
52
删去分组
54
退出
是
56
输入地址至表内
44
可靠源？
否
58
将分组注释为来自IP源及
设置其分组收到标志
是
60
将IP源的最近
分组计数增量
46
接收分组
48
退出
62
将总分组计数增量
64
最近分组
计数超过阈值否？
是
66
删去分组
否
70
总分组计数
超过阈值否？
否
是
68
退出

图 4

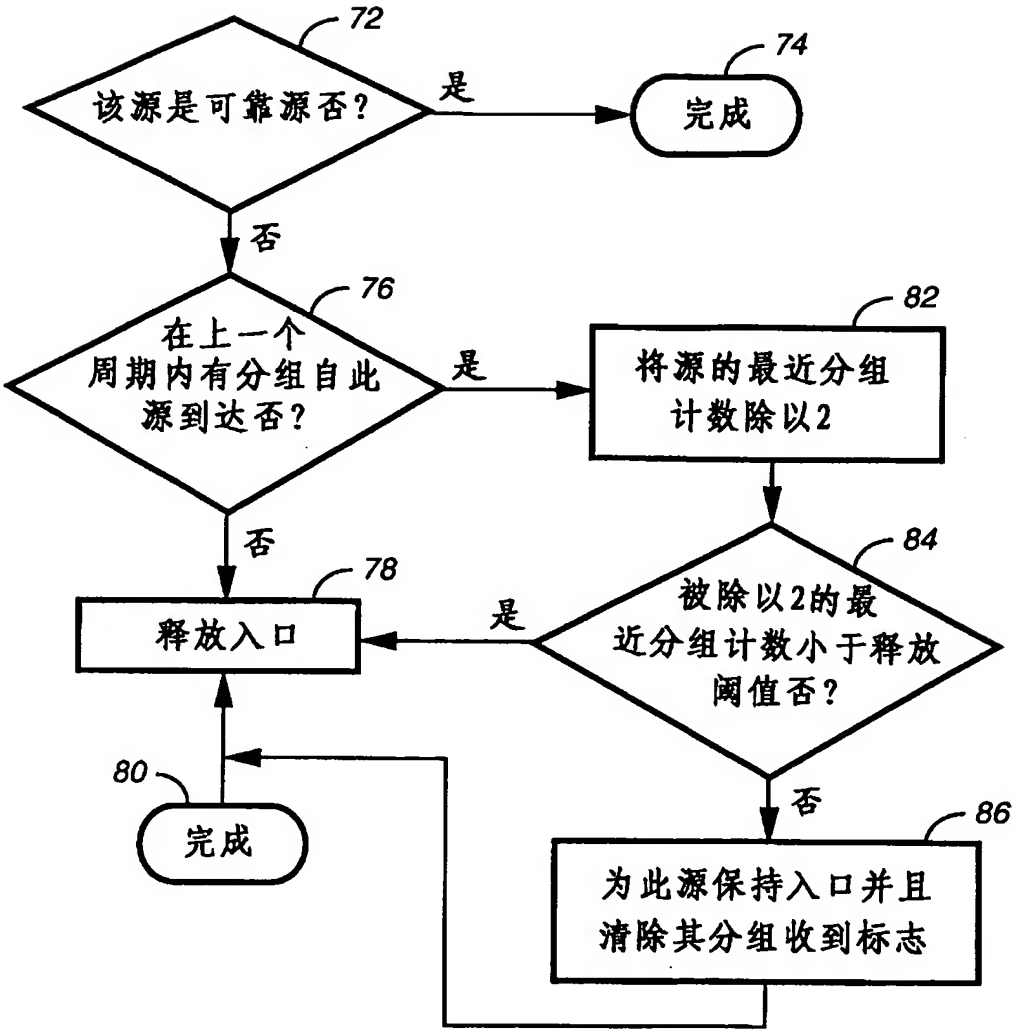

72
该源是可靠源否?
是
74
完成
否
76
在上一个周期内有分组自此源到达否?
是
82
将源的最近分组计数除以2
否
84
被除以2的最近分组计数小于释放阈值否?
是
78
释放入口
80
完成
否
86
为此源保持入口并且清除其分组收到标志

图 5